Published and Copyright (c) 1999 - 2011
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1303 01/21/10

~ Cybercrime Global Shift ~ People Are Talking! ~ Apple Without Jobs?
~ Nintendo 3DS in March! ~ iPad Hackers Charged! ~ 100 Trillion Emails!
~ Search Engine Spam Rise ~ Verizon Challenges FCC ~ AV Scam on Twitter!

~ World Running Out of IP ~ McDonald's Phish Scam! ~ Java Attacks on Rise!

-* Final Fantasy XIII-2 in '12! *-
-* Guinness Releases Wacky Game Records *-
-* FCC Net Neutrality Decision Will Hit Court *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Wasn't it just last week that I surrendered to Mother Nature? Apparently she didn't see my white flag because it blended in so well with all of the snow we have sitting on the ground! And since then, we've had two more storms, adding over another foot or so of more snow! This is turning into a season of the ridiculous! During the storm earlier this week, I was using our snow thrower. I happened to take a step backward, and my heel hit a patch of ice. Holding onto the snow thrower's handles didn't help me keep my balance, and I went down like a sack of bricks, landing on my tail bone. That was the most excruciating pain I have ever felt! I thought that I was going to pass out. I managed to limp to my car and sat down for a bit until the pain subsided. I'm still sore!

And then another storm today! I got a call from work early this morning. Because the storm was hurting business, managers were told to cut some staff hours. I now had the day off. Oh boy, now I had plenty of time to clean up more snow! I spent most of the day clearing snow, and made two passes of everything. As I finished, the sun emerged and the snow stopped! Finished a couple of errands, and then collapsed for the rest of the afternoon! Needless to say (but I am), I'm spent!

So, that's how my week went around here. It's been otherwise quiet on the news front, and not much time available to consider some hot topics to discuss in my editorial. So much for some positive changes so far in this new year!

Until next time...

=~=~=~=

PEOPLE ARE TALKING
compiled by Joe Mirando
joe@atarinews.org

[Editor's note: Due to work-related time constraints, there will not be a People Are Talking column this week.]

=~=~=~=

->In This Week's Gaming Section - Nintendo 3DS Out in March!
Final Fantasy XIII-2 Coming Next Winter!
Guinness Releases Wacky Videogame Records!
And more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!

Nintendo 3DS To Cost $250, Out March 27 in US

Promising to usher in a new era in 3-D entertainment, Nintendo says its glasses-free handheld 3DS will go on sale on March 27 in the U.S. for $250. That's the same price that the revolutionary Wii console cost when it went on sale in 2006.

The president and chief operating officer of Nintendo of America, Reggie Fils-Aime, said Wednesday the 3DS is a "truly unique experience that doesn't exist anywhere else."

"This is a different kind of 3-D. Something you haven't experienced before. Not in theaters, not at trade shows." Fils-Aime told a crowd of journalists, bloggers and analysts in New York City. "Of course, there are no glasses."

The gadget features a touch screen on the bottom and a 3-D screen on top. It has three cameras, one facing the user and two facing outward. The latter two let you take 3-D photos, which can be instantly displayed on the screen. There's also an accelerometer and a gyroscope. These track players' movements and how they tilt the screen, so they can play games with motion-based capabilities or see the 3-D games from different angles.

A "Mii Creator" uses photos you take of yourself to instantly create a cartoon avatar based on your image. Then you can adjust it as you like.

The 3DS includes new social features, including "StreetPass," which lets users exchange game information with other 3DS users nearby. For example, your Mii avatar or game high scores can appear on your friend's 3DS if they have also chosen to activate this feature.

Nintendo Co. said more than 30 games will be available for the 3DS by early June. Games will range from "Nintendogs + Cats," which adds feline companions to the popular puppy simulator to "The Legend of Zelda: Ocarina of Time 3D" to 3-D versions of EA's Madden NFL Football" and Capcom's "Resident Evil: The Mercenaries." Older games, including those for the original Game Boy, will be available for download.

The 3DS will be available in black and shiny aqua blue. It can play games from older DS systems, but they just won't be in 3-D. The 3-D gradient is adjustable on the 3DS, or it can be turned off completely. If your eyes don't adjust to the 3-D screen immediately, it helps to start out the games in 2-D mode and then slowly turn up the 3-D slider.

Nintendo recommends that children aged 6 or younger should not play 3-D games because it could affect the development of their vision, similar to warnings issued by makers of other 3-D products.

But the American Academy of Ophthalmology says there are currently no conclusive studies on the short- or long-term effects of 3-D products on children's eye development or vision health. At the same time, if a healthy child develops headaches or can't see 3-D images, this could be a sign of an eye disorder, the group said in a statement this week.

Final Fantasy XIII-2 Coming Next Winter

Game developer Square Enix on Tuesday announced a new version of Final Fantasy for the PlayStation3 and Xbox 360 game consoles.

Dubbed "Final Fantasy XIII-2," the game will be available next winter. Rumors about this second installment of XIII made the rounds recently thanks to the Web domain registration of Finalfantasy13-2game.com.

"Production on Final Fantasy XIII-2 is underway, and builds upon the best aspects of Final Fantasy XIII," Square Enix said in a statement. "In particular, a brand new story and evolved battle system promise to stand out markedly against the standard for high-quality content established by the previous title."

The company also released a screenshot entitled, "Why does mankind defy its fate?" and a low-res video (below) of some gameplay has shown up on YouTube in Japanese. Square Enix claims that the game series has shipped over 97 million units worldwide as of September 2010, with XIII accounting for 6 million units. The game has not yet been rated by the ESRB.

Duke Nukem Forever to Finally Ship Year Before World Ends

Everyone knows the world ends in 2012, so why not send if off in style, kicking butt and chewing bubble gum?You do still chew bubble gum, don't you?

That's right, Duke Nukem Forever will finally be with us, for better or worse, on May 3, 2011 (May 6, 2011 worldwide). Publisher 2K Games and pinch-developer Gearbox Software (Borderlands, Brothers in Arms) announced the date this morning. The presumably irreverent first-person shooter will ship simultaneously for Xbox 360, PlayStation 3, and Windows PCs.

Is it really "the moment fans all over the world have been for"? I think we're all a little sour on Duke these days, given 3D Realms' monumental failure to bring a sequel to market in anything like a timely fashion.

The only thing weirder than 3D Realms' inability to capitalize on killer IP has been everyone else's inability to. How many first-person shooters the last decade or so have the kind of zany combat antics (like shrink rays, foot-stomps-of-death, and freeze rays) that Duke Nukem 3D did?

Anyway. Check out the new trailer, which I'd call kind-of-safe-for-work (depending).

What else. The press release confirms all the stuff you'd expect from a proper Duke Nukem game. Like: Invading alien hordes, pig cops, alien shrink rays, mammoth alien bosses, women in distress, naked pole-dancers, adult magazines, whiteboards you can doodle on, outlandish weapons, and other forms of bad-assery. Yep, welcome back to gaming-as-juvenile-pasttime.

2K Games says to expect a demo at some point. If you want it early, you'll have to join the Duke Nukem Forever First Access Club, which means spending extra cash up front: The access codes are only available in Gearbox's Borderlands: Game of the Year Edition.

Guinness Releases Wacky Videogame Records

The most perfect virtual bowler, the most swearing in a videogame and the most popular game on Facebook are just some of the records listed in the 2011 gamer's bible of wacky achievements from Guinness World Records.

The new "Guinness World Records 2011 Gamer's Edition" published on Thursday features an array of record holders from pensioners to schoolchildren, demonstrating the extent to which people from all walks of life have embraced videogames.

"Gaming has become a hugely important part of popular culture and this year's Gamer's Edition reflects just that," said Guinness World Records Gaming Editor Gaz Deaves.

The oldest gamer to make the book is 85 year-old John Bates from Onalaska, Wisconsin. The former high school principal became hooked on Nintendo's Wii Bowling and went on to achieve the Most Perfect Games on Wii Sports Bowling (2,850).

At the other end of the age spectrum is nine-year-old Ryota Wada from Tokyo, who has been recognized as the Youngest Gamer to Achieve a Perfect 'AAA' score on music videogame Dance Dance Revolution.

Mitsugu Kikai, 25, from Tokyo is recognized for having the largest collection of memorabilia related to videogame character Super Mario (5,400 individual items) and Annie Leung from San Francisco is featured for achieving the highest score on Guitar Hero 3 for a female (789,349 points).

Other records include the most swearing in a videogame, the most people to sing to a karaoke videogame and the most popular game on Facebook, which is FarmVille with 60 million monthly active users.

The book also contains the results of a poll conducted by Guinness World Records to find the best videogame character.

More than 13,000 gaming fans voted and chose Mario, the good-natured mustachioed Italian plumber as the top character.

Second spot went to Link from the popular Legend of Zelda series, and third went to the genetically engineered super soldier, Master Chief, who made his first appearance a decade ago in Halo: Combat Evolved (Microsoft, 2001).

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

FCC Net Neutrality Decision Sets up Court Battle

The U.S. Federal Communications Commission's recent vote to impose net neutrality rules on broadband providers will lead to lengthy court battles, as well as efforts in Congress to repeal the rules, a group of Internet law experts said Wednesday.

Even supporters of the FCC's Dec. 21 vote predicted that multiple court challenges are likely as soon as the FCC officially publishes the new rules in the Federal Register. Court challenges to the rules are "inevitable," said Colin Crowell, former senior counselor to FCC Chairman Julius Genachowski .

Multiple lawsuits in courts across the U.S. are likely, with some questioning the FCC's authority to make rules affecting Internet service providers and other groups suggesting the rules are arbitrary, added Markham Erickson, executive director of the Open Internet Coalition and a supporter of the rules. The new rules prohibit service providers from selectively blocking or slowing Web traffic.

None of a panel of four Internet law experts speaking at the Congressional Internet Caucus' State of the 'Net conference explicitly predicted the outcome of the lawsuits, although Larry Downes, a technology author and fellow at the Stanford Law School Center for Internet and Society, suggested that the courts or Congress would make changes.

"This was an effort by the FCC to punt this down the road, both to the courts, because the legal challenges are inevitable, and to Congress," he said. The net neutrality vote was an effort to get the issue "off their plate, so they can move on to some more important issues."

While the panel seemed to agree on the possibility of lawsuits, they said the prospects of congressional action are less certain. Representative Marsha Blackburn, a Tennessee Republican, predicted Tuesday that Congress would repeal the net neutrality rules, but it's unlikely that President Barack Obama, a longtime supporter of net neutrality rules, would sign the repeal, panelists said.

Asked why House of Representatives Republicans plan to push a repeal even if it won't succeed, Christopher Yoo, director of the University of Pennsylvania Law School Center for Technology, Innovation and Competition, said that lawmakers will use the repeal effort to show voters they are against this type of regulation. "It's good politics," he said.

The net neutrality vote at the FCC may also set up a long-term effort to rewrite the Telecommunications Act of 1996 for the Internet Age, Yoo said. Congress and the FCC should "tread lightly and carefully" when exploring new rules for the Internet because of rapid changes in technology, including a fast move by Internet users to mobile broadband, Yoo added.

Court action on the net neutrality rules may preempt any congressional action, said Crowell, founder of Crowell Strategies, a public policy consulting firm. He'd rather see Congress focus on other issues, such as clearing spectrum for mobile broadband and reforming the Universal Service Fund, which subsidizes traditional telephone service, he said.

Yoo agreed, saying that the net neutrality debate was less important than spurring broadband competition and implementing the FCC's national broadband plan, released last March. The net neutrality debates in recent years "probably generated much more attention than they deserved," he said. If broadband competition was "robust enough, all these issues would go away," he added.

Verizon Challenges FCC's Net Neutrality Rules

Verizon Communications Inc. on Thursday filed a legal challenge to new federal regulations that prohibit broadband providers from interfering with Internet traffic flowing over their networks.

In a filing in federal appeals court in the District of Columbia, Verizon argues that the Federal Communications Commission overstepped its authority in adopting the new "network neutrality" rules last month.

The rules prohibit phone and cable companies from favoring or discriminating against Internet content and services - including online calling services such as Skype and Internet video services such as Netflix, which in many cases compete with services sold by companies like Verizon.

The FCC's three Democrats voted to adopt the rules over the opposition of the agency's two Republicans just before Christmas. Republicans in Congress, who now control the House, have vowed to try to block the rules from taking effect. They argue that they amount to unnecessary regulation that will discourage phone and cable companies from investing in their networks.

Several key House Republicans, including House Commerce Committee Chairman Fred Upton of Michigan, welcomed Verizon's actions Thursday as "a check on an FCC that is acting beyond the authority granted to it by Congress." The court challenge had been widely expected.

In a statement, Verizon said that while it is "committed to preserving

an open Internet," it remains "deeply concerned by the FCC's assertion of broad authority for sweeping new regulation of broadband networks and the Internet itself."

The company is taking the case to the same federal court that ruled last year that the FCC had exceeded its legal authority in sanctioning cable giant Comcast Corp. The agency had cited Comcast for discriminating against online file-sharing traffic on its network - violating broad net neutrality principles first established by the agency in 2005. Those principles served as a foundation for the formal rules adopted by the commission last month.

Last year's court ruling forced the FCC to look for a new framework for regulating broadband to ensure the commission would be on solid legal ground in adopting net neutrality and other rules. The agency currently treats broadband as a lightly regulated "information service," as opposed to phone service, which is more heavily regulated as a so-called "common carrier."

At one point, FCC Chairman Julius Genachowski proposed redefining broadband as a telecommunications service subject to common carrier obligations to treat all traffic equally. But he later backed down in the face of fierce opposition from the phone and cable companies, as well as many Congressional Republicans.

And he now argues that the agency has ample authority to mandate net neutrality under the existing regulatory framework for broadband - an assumption that will be tested in the Verizon challenge.

A senior FCC official said Thursday that the agency is confident that its new net neutrality rules are legally sound and is prepared to defend them.

The rules represented an attempt to craft a compromise on an issue that has divided the telecommunications and technology industries. On one side, Internet companies such as Skype, as well as public interest groups, argue that strong rules are needed to prevent broadband providers from becoming online gatekeepers that can dictate where people go and what they do online.

But the big phone and cable companies insist that they need flexibility to manage Internet traffic to keep their networks running smoothly and preventing bandwidth-hogging applications from slowing down their systems. They also maintain that they should be able to charge extra for special services over their broadband lines and earn a healthy return on the billions of dollars they have spent on network upgrades.

New York-based Verizon is the country's fourth-largest fixed-line Internet service provider, with 8.3 million subscribers. It's investing more in home broadband than any other company, since it's upgrading about two-thirds of its local-phone network with optical fiber for ultra-fast Internet access.

The regulations adopted last month try to find a middle ground. The rules require broadband providers to let subscribers access all legal online content, applications and services over their wired networks. But they give providers flexibility to manage data on their systems to deal with network congestion and unwanted traffic, including spam, as long as they publicly disclose how they manage the network.

The new rules do prohibit unreasonable network discrimination - a category that would likely include "paid prioritization," which favors the broadband providers' own traffic or the traffic of business partners that can pay extra - but they do not explicitly bar the practice.

The regulations also prohibit wireless carriers from blocking access to any websites or competing services such as Internet calling applications on mobile devices, and they require carriers to disclose their network management practices, too. But they give wireless companies more flexibility to manage data traffic because wireless systems have less network bandwidth and can become overwhelmed with traffic more easily than wired lines.

A Global Shift in Cybercrime

Research from SpiderLabs found that malicious tools became more customized, automated and persistent in 2010. This trend combined with the popularity of mobile devices and social media is providing the perfect recipe for cybercriminals looking to compromise business, customer and user private and sensitive information.

Key findings:

* Food and beverage regained its title as the most breached industry-representing 57% of the investigations.
* Third-party vendors continue to put companies at risk-88% of breaches resulting from insecure software code or lax security practices in the management of third-party technology.
* Cybercriminals got fresh in 2010-because in-transit credit card data is usually more recently created (more fresh) than stored data, 66% of investigations found the theft of data in transit.
* A single organized crime syndicate may be responsible for more than 30% of all 2010 data breaches.

Among the most interesting and surprising elements of the report is the rate and sophistication of attacks against mobile platforms and social networking sites. As the security of mobile networks has improved, mobile devices are increasingly the target of attacks, while social networking sites are quickly becoming cybercriminals' platform of choice to expand and propagate destructive botnets. Drive-by infections and mobile phishing attacks were among the most popular client-side attacks in 2010.

Geolocation data is helping cybercriminals launch more sophisticated and targeted attacks against social networks. Mobile devices offer cybercriminals an open door to corporate authentication credentials, sensitive data and trade secrets.

Anti-virus software is losing the battle against malware - the new breed of malware is virtually undetectable by current scanning software.

Top strategic security initiatives for 2011

A key take-away from the report is that attacks are often successful in organizations that believed a comprehensive data security strategy was in place. For executives and managers who are tasked with ensuring their company does not suffer a security event, the report offers specific guidance for 2011.

* Assess, reduce and monitor client-side attack surface: Monitor and inventory applications to measure adherence to standards and evaluate risk.
* Embrace social networking, but educate staff: An established policy and education can help protect against attacks originating from social networking tools.
* Develop a mobile security program: Gaining control over configurations of mobile devices will help reduce risk.
* Enforce security upon third party relationships: Choose a platform and vendor with a solid security history, and require vendors to undergo third-party security testing.

Zeus Malware Now Targets Online Payment Providers

The move mirrors the evolution of card fraud in the 1980s and 1990s, when fraudsters initially targeted banks for cash advance fraud, then, as the banks developed their internal anti-fraud resources, moved over to quasi-cash platforms such as foreign currency purchases and then over to retail and e-tail sales outlets.

The parallels between card fraud evolution and the evolution of Zeus is reflected in the attack vectors against a few websites Trusteer researchers have identified as being targeted.

Money Bookers is an online payment provider allowing you to make online payments without submitting your personal information each time. We have found 26 different Zeus configurations targeting Money Bookers.

This usually indicates that fraudsters have a solid business around this target. For comparison, this number doesn t fall short of some of the highly targeted banks and brands in the world. For those of you who don t know what a Zeus configuration file is - it s basically a set of instructions that Zeus gets on which websites to target and what to do with them (steal login credentials, tamper with HTML webpages, etc). Different configurations represent different work efforts of targeting online websites.

Another interesting target is Web Money. This is another online payment solution that claims to have more than 12 million active users. Web Money is targeted by 13 different Zeus configurations, with the last one released January 16th, indicating that this is hot target for fraudsters. As with all the other online payment providers, Zeus steals login information and other sensitive information of Web Money users.

Another popular target is Nochex, a UK based online payment company specializing in smaller online businesses. Nochex is targeted by 12 different Zeus configurations with the last one released in January 16th.

While these three examples represent online payment providers which have been targeted for months, there are new comers as well. One example is netSpend. This website has been recently started to be targeted by Zeus. netSpend is a prepaid card provider. You add money to your account and use you netSpend account to pay online.

The last example for today is e-gold which provides a money-like currency and wire transfer services. This website has been indicted in the past for violating money laundering regulations. This website is targeted by 16

different Zeus configuration. Could it be that fraudsters are targeting other fraudsters?

The genuine login page for e-gold asks the user for the account number, passphrase and uses CAPTCHA technology to help prevent automated attacks.

On a Zeus-infected machine (with an e-gold targeting configuration), the malware injects an additional element into the login page that requests the alternate password - plus the email associated with the account, which can then presumably be tapped for back-door access to the account.

The following screenshot shows the login page after it has been tampered with by Zeus (the injected fields are identified using a red rectangle):

Trusteer believes this trend of targeting online payment providers will continue as more retailers allow these alternate payment methods with their Web sites.

What can be done to counter the problem of Zeus-enabled credential fraud against a diversified range of online payment providers?

Customers of all sites where purchases are involved need to protect their PC or access terminal, using secure browsing services and solutions that specialize in protecting online payments and online banking.

Users should also avoid using public access computers, as well as computers you do not own and therefore have direct control over.

Retailers and payment providers, meanwhile, need to assess the risk associated with their customers' endpoint devices. They should, we believe, reject transactions from accounts used over insecure endpoints.

Two Hackers Charged with Stealing iPad Data

Two hackers were charged Tuesday with breaking into the AT&T mobile network and stealing data from 120,000 users of Apple's iPad tablet computer, including several celebrities, US officials said.

Andrew Auernheimer, 25, of Fayetteville, Arkansas, and Daniel Spitler, 26, of San Francisco, were taken into custody by the FBI and charged with "conspiracy to hack AT&T's servers and for possession of personal subscriber information," the Justice Department said.

If convicted, they could face up to five years in prison and hefty fines.

Officials said both suspects were members of Goatse Security, described as "a loose association of Internet hackers and self-professed Internet 'trolls'" who look for security flaws in computer networks.

According to a criminal complaint, they were able to access the network between June 5 and 9, 2010 to obtain email data and other information from some 120,000 iPad users.

An article by the news website Gawker.com, which was cited in the complaint, said the breach "exposed the most exclusive email list on the planet," including the addresses of ABC News correspondent Diane Sawyer, New York Mayor Michael Bloomberg and former White House chief of staff

Rahm Emanuel.

"Hacking is not a competitive sport, and security breaches are not a game," said the US attorney in New Jersey, Paul Fishman.

"Computer intrusions and the spread of malicious code are a threat to national security, corporate security, and personal security."

Microsoft Donates Security Tools

Hacker conferences are often forums for revealing, and learning about, the latest security exploits and techniques, not the least the Black Hat Technical Security Conference 2011, which is being held this week in Washington, D.C.

Such events can also serve as a way to distribute free products to help corporate security personnel better police their domains. That's what Microsoft is doing at this year's Black Hat D.C. conference .

Microsoft quietly announced this week that it has released betas of three updated security testing tools, targeting security professionals and ISVs in an attempt to encourage development of less vulnerable software.

First up is a version of a tool that Microsoft says it has used internally for the past five years.

"The Attack Surface Analyzer beta is a Microsoft verification tool now available for ISVs and IT professionals to highlight the changes in system state, runtime parameters and securable objects on the Windows operating system," said a post to Microsoft's Security Development Lifecycle (SDL) blog, Monday.

"This analysis helps developers, testers and IT professionals identify increases in the attack surface caused by installing applications on a machine ... The tool also gives an overview of the changes to the system Microsoft considers important to the security of the platform and highlights these in the attack surface report. "

Microsoft also released a beta of version 3.1.6 of its SDL Threat Modeling Tool, which enables developers to perform early, structured analysis and "proactive mitigation of potential security and privacy issues in new and existing applications," another post to the same blog said.

The updated threat modeling tool now supports Microsoft's Visio 2010 for designing diagrams.

Meanwhile, a third tool, called the BinScope Binary Analyzer 1.2, also debuted in beta at Black Hat, adding compatibility with the latest release of Microsoft's development environment, Visual Studio 2010.

"The BinScope tool is available in two forms: a stand-alone version and as an add-on that integrates fully with Visual Studio," the post said. "In addition, it integrates with Microsoft Team Foundation Server 2008 and Microsoft Team Foundation Server 2010 to output results into work items."

Both the threat level tool as well as the binary analyzer are due to ship in final form this fall. Microsoft did not give a general availability date for the attack surface analyzer.

Beyond that, Microsoft announced that beginning on Feb. 21, it will start offering SDL consulting services.

Of course, Black Hat rarely goes by without one or more controversies popping up.

For instance, a German security specialist planned to give attendees code that they can run on high-performance cloud computer systems to help them break Wi-Fi passwords using massive computer power available for a few dollars.

Additionally, at last winter's conference, a security researcher disclosed a zero-day vulnerability in Internet Explorer.

Can Apple Thrive Without Its Visionary CEO?

If investors were as visionary as Steve Jobs has provedto be during his 35 years of tech wizardry, they might be able to figure out whether Apple can still thrive if its founder and CEO doesn't return from his indefinite medical leave.

But Jobs' prescience is a rarity, which is why doubt and anxiety will probably hang over the company until his fate is clearer.

The iPod-iPhone-iPad revolution that Jobs unleashed over the past decade should ensure that Apple's revenue and earnings keep growing for at least the next two to three years, according to analysts. What's more, Jobs has assembled and trained a savvy, hard-driving management team that should be capable of following his road map for the company.

The question is whether Apple can remain a step ahead and develop products that reshape technology, media and pop culture if Jobs isn't around to divine the next big thing.

Without Jobs, "Apple is a lot more like other companies. Its extraordinariness fades," says technology analyst Roger Kay of Endpoint Technologies Associates.

Apple Inc. announced Monday that Jobs, who co-founded the company in 1976, would take an indefinite medical leave for unspecified problems. The leave could be related to his previous bout with pancreatic cancer or his 2009 liver transplant.

For now, investors appear to be hoping for the best. Apple stock fell $7.83, a little more than 2 percent, to close Tuesday at $340.65. It recovered more than half of that loss after the closing bell after reporting strong earnings.

For the regular trading day, Apple lost $7 billion in market value, although most analysts believe Jobs' leadership and presence is worth much more to the company.

Jobs' value is difficult to gauge because of the sheer force of his

personality, said Robert Sutton, a professor of management science at Stanford University who has studied Jobs and Apple. "Anyone who thinks they can estimate that is probably lying," Sutton says.

Stock market analyst Brian Marshall of investment bank Gleacher & Co. suspects people still hope Jobs will return to the CEO job that he has held since 1997. Since then, Jobs has orchestrated a turnaround that increased Apple's market value by 100 times.

Marshall and other analysts aren't optimistic that Jobs will resume his CEO duties, partly because he did not set a timetable for his return. Before he got the new liver, Jobs took a leave of absence from January through June 2009.

It's tough to gauge Jobs' current health problems because he has said so little about his past ones. He had a tumor removed in 2004 - a rare and very treatable form of pancreatic cancer - but never said whether it had spread to lymph nodes, nor how extensive his surgery was.

"We don't really know how much of his pancreas was removed. He may just have a remnant," and that may be causing continued digestive difficulties, said Dr. Charles R. Thomas of Ohio State University's Knight Cancer Institute.

Dr. Jennifer Obel, a spokeswoman for the American Society of Clinical Oncology and a cancer specialist at Northshore University Health System in suburban Chicago, said the prognosis is good for those with pancreatic tumors like the one Jobs had, even if the tumors spread.

"He's done extremely well living with this disease for many years," she said. "I wouldn't assume anything until he has released more information."

Apple declined further comment Tuesday on Jobs' health.

Apple barely missed a beat the last time Jobs was gone, and its stock climbed more than 60 percent as sales of the iPhone and Mac computers surged, even as the recession dragged on. That's a testament to Apple's chief operating officer, Tim Cook, who will be in charge while Jobs is away once again.

In a Tuesday conference call to discuss Apple's earnings, Cook predicted Apple will still shine.

"Apple is doing its best work ever," Cook said. "We are all very happy with the product pipeline, and the team here has an unparalleled breadth and depth of talent and a culture of innovation that Steve has driven in the company. Excellence has become a habit."

Cook has pretty much the same management team supporting him this time. The key players besides Cook include Jonathan Ive, who oversees the elegant design of Apple's products; Ron Johnson, who runs Apple's stores; Philip Schiller, the marketing chief; and Scott Forstall, who supervises the iPhone software.

It's a bench that investors would like to know better, says Jeffrey Sonnenfeld, a professor at the Yale School of Management and an expert on executive leadership.

"You only hear about Santa," he says, "but it's time that we hear more about the elves."

Cook, who has been with Apple since 1998, and Ive, who has been with there since 1992, will probably carry the biggest load while Jobs is gone, analysts say.

Partly because his role at Apple attracted so much attention during Jobs' last medical leave, Cook is better known than Ive. Apple has recognized Cook's contributions by making him its top-paid executive, with a 2010 compensation package valued at $59.1 million. Jobs limits his annual salary to $1.

But Ive has played a critical role in turning the products that Jobs envisioned into reality, said Leander Kahney, who has written books and a blog about Apple.

Apple's management team has been working together for so long that all the key executives should have a sense of what Jobs would want. And they may still be in touch with Jobs on key decisions because Jobs said he intends to remain involved in the company's strategy. Kay thinks Jobs may have planned even more in the past year than he usually does because of his shaky health.

The stakes are much higher than during Jobs' last medical leave. When Jobs left last time, Apple's market value stood at about $78 billion. It is now $312 billion, behind only Exxon Mobil among U.S. companies. Apple also is facing fiercer competition from Google, which has already threatened the iPhone with a rival software system for smart phones and is now setting its sights on the iPad in the market for tablet computers.

Jobs' greatest gift hasn't been for invention as much his uncanny ability to anticipate what people want and then demand the technology be designed in a simple way that appeals to a mass market.

"You can't really teach that," said George Haley, a business and marketing professor at the University of New Haven. "You can teach the processes, but not the insight. It takes a genius to do it right."

Jobs has also shown an exquisite sense for when the time is right for a product. For instance, the concept for what turned into the iPad was brought to Jobs several years before Apple had even introduced its own phone. Jobs liked the idea of a computer tablet but decided instead that its touch-screen technology would be better suited for a smaller screen at that time. That decision hatched the iPhone in 2007, a hot-selling device that paved the way for Apple's latest must-have gadget, the iPad.

Other companies developed the technology that created the computer mouse and digital music players, but neither of those innovations caught on until Jobs embraced the ideas and turned them into game-changing products.

"Steve did not invent MP3 players - he reinvented them," said Tim Bajarin, the president of Creative Strategies and a longtime Apple watcher. "He didn't invent the smart phone - he reinvented it. He didn't invent the tablet - he reinvented it."

It's difficult to put a price on that kind of market intuition, particularly in an industry that changes so quickly. Almost no one had heard of Twitter three years ago or Facebook five years ago - or for that matter the iPod 10 years ago.

Many analysts liken Jobs to Walt Disney, an entrepreneur who didn't come

up with animation or amusement parks but sculpted them into a business that left an indelible mark on the world. Jobs is now the largest shareholder of Walt Disney Co., a stake he accumulated when he agreed to sell Pixar Animation a few years ago.

Just as Walt Disney Co. survived the 1966 death of its founder, Apple looks to be positioned well if Jobs doesn't return to health. But even Disney struggled for years after the well of its founder's ideas finally ran dry.

Search Engine Spam on the Rise

If you've noticed lately that Google's search results are a bit spammy, you're not alone.

In a blog post, Google Principal Engineer Matt Cutts acknowledged that "we have seen a slight uptick of spam in recent months," and that tech watchers are growing critical. Cutts then outlined a few new initiatives to improve the quality of Google's search results.

Among them: Google has a new "document-level classifier" that's better at detecting the hallmarks of spam, such as oft-repeated keywords; Google is improving its ability to detect hacked sites, which were a big source of spam last year; and the company is evaluating other changes, including a crackdown on Websites that primarily copy other sites' content.

But on the issue of "content farms," Cutts didn't have all the answers. If you're not familiar with the term, you've probably stumbled upon some content from purveyors. For example, many in the media call sites Demand Media and AssociatedContent content farms. Rich in search keywords and produced on the cheap, content from these sites appears prominently in search results but seem geared solely towards appeasing search algorithms.

Although Google tweaked its algorithms last year to give content mills less prominence, the problem hasn't gone away, and Cutts' blog post offered no further solutions. "The fact is that we're not perfect, and combined with users' skyrocketing expectations of Google, these imperfections get magnified in perception," he wrote. "However, we can and should do better."

Cutts reiterated that Websites don't get preferential treatment by purchasing or displaying Google ads. Their rankings don't improve and they're just as likely to be punished for violating Google's quality guidelines.

I suppose it's comforting to hear Google address issues of search quality, especially as criticism grows louder. Notably, new search competitor Blekko has created a spam clock to count how many spam pages have been created since the start of the year. Google says its results have half the spam they did five years ago, but that count is meaningless if low-quality content mills are able to game the system and get high page rankings.

With Google co-founder Larry Page stepping up to chief executive, the pressure's on to improve search while cultivating newer ventures such as software and social networking. Hopefully Cutts' blog post is just the

beginning.

Twitter Targeted With Fake Antivirus Software Scam

Twitter has been resetting passwords for accounts that started distributing links promoting fake antivirus software in an attack that used Google’s Web address shortening service to conceal the links’ destination.

The links, masked by Google "goo.gl" URL shortener, bounce through a series of redirect URLs before landing on a Ukrainian top-level domain that then redirects to an IP address associated with other fake antivirus software scams, wrote Nicolas Brulez of Kaspersky Lab on a company blog.

Victims landing on the fake antivirus software page are prompted to scan their computer. If they approve the scan, the page asks if they want to remove threats from their computer: doing so starts the download of a bogus security program called "Security Shield."

Fake antivirus programs remain a pervasive problem on the Internet, with hundreds of variations. The applications target Windows users, and the programs are often installed by exploiting vulnerabilities in a computer’s software. Once installed, the applications badger users to pay for a full version of the program. Many of the programs are totally ineffective at actually removing malware from a computer.

Del Harvey, head of Twitter’s Trust and Safety Team, wrote on her Twitter account that "we’re working to remove the malware links and reset passwords on compromised accounts."

"Did you follow a goo.gl link that led to a page telling you to install ’Security Shield’ Rogue AV?" she wrote. "That’s malware. Don’t install."

Although Brulez classifed the attack as a worm, implying it spreads from account to account, Harvey said the issue was not related to a worm.

If the problem isn’t spreading between Twitter users, that raises the question of how the attack began.

One possibility is that it is related to an attack on Gawker Media in December. In that incident, the e-mail addresses and passwords for registered users of the media company’s Web sites were pilfered by a group called Gnosis. Twitter saw a raft of spam after the Gawker hack, as it is believed that many users used the same password for the Web sites, which made their Twitter accounts vulnerable.

Sunbelt Software, a security vendor now owned by GFI Software, provides detailed instructions of how to remove the Security Shield fake antivirus program in one of its forums.

McDonald’s Phishing Scam: I’m Not Lovin’ It

An e-mail is circulating that appears to be some sort of survey from

McDonald’s along with the promise of a $250 reward for participating. While it would be awesome to get an easy $250 just for letting McDonald’s know they have the best French fries of any fast food chain, or that you wish the McRib would be added to the permanent menu, this is really just a phishing scam.

The scam is very similar to another recent phishing scam involving Coca Cola. In fact, the two are almost certainly from the same attacker(s) and were most likely developed simultaneously. AppRiver’s Fred Touchette noted something interesting on the Coca Cola phishing e-mails. "One interesting note about this page though is that upon inspecting all of the links on the page I noticed that most of them do in fact link to the Coke website however, four of them at the end in yellow actually link to McDonald’s websites. This is either a sign that this phishing page is being recycled from an old McDonald’s scam, or it was part of a misconfigured phishing kit."

In a post humorously titled "Fillet O’ Phish", AppRiver’s Troy Gill describes the phishing scam. "The messages appear addressed from McDonalds Consulting and urge you to follow a link to take the survey. There are only 5 questions that you must answer before you receive your $250 reward. Once you click to submit your answers you are taken to a page that requests your personal information along with your credit card number so that they can "credit your account" the $250 reward."

These McDonald’s phishing e-mails have the McDonald’s logo, color scheme, and "I’m Lovin’ It" tag line emblazoned across the top which give it some semblance of legitimacy. However, there are many obvious issues with the message that should be major red flags.

First of all, the message starts out explaining that it is a "public opinion poll conducted by McDonald’s, a non-partisan polling organization." Well, McDonald’s is a lot of things, but it is not a polling rganization - non-partisan or otherwise.

The biggest red flag, though, should be the part where the survey requests your credit card information so they can deliver your $250 reward as a credit to your account. How exactly would McDonald’s deliver on the promised $250 reward for survey takers who don’t have a credit card? Better yet, when - in the history of either surveys or credit cards--has any organization asked for your credit card information so it could credit your account?

No. It doesn’t work that way. If it were legitimate, McDonald’s would issue McDonald’s gift cards, or at least some sort of Visa or Mastercard gift card to fulfill the reward, and it would be some sort of drawing - not a scenario where McDonald’s is just randomly giving $250 to everyone with an e-mail account who takes 30 seconds to answer a couple questions.

If it’s too good to be true, it probably is.

Java Attacks on the Rise As Spam Declines

For years, the scourge of the Internet has been ever increasing volumes of spam that clog inboxes around the world. According to a new report from Cisco, 2010 was the first year on record that spam volumes actually

declined.

Cisco’s report also points out some counter-intuitive data about which types of technologies are being attacked. As opposed to Adobe PDF which had been a top target, Cisco said that Java vulnerabilities are now more exploited than those in Adobe Acrobat and Reader. Overall, Cisco is rating the status of cybersecurity threats at the end of 2010 at a level lower than they were in 2009, though there is still cause for concern.

The decline in spam volumes varies by geography according to Cisco. In the U.S., spam volume decline by 1.6 percent in 2010 in comparison to 2009. That said the U.S. still continues to lead globally in terms of spam with 11.1 trillion spam messages sent in 2010, down from 11.3 trillion sent in 2009. Among the other countries that experienced spam declines were Brazil with a 47.5 percent drop and Turkey which declined by 87 percent.

Mary Landesman, senior security researcher at Cisco, told /InternetNews.com/ that the decline in spam volumes in 2010 was due to 8 major takedowns of spam senders. She noted that one of the biggest spam farms that was removed in 2010 was an affiliate marketing facilitator that was linked to pharma spam. Landesman said that by taking down the affiliate engine, the revenue stream for the pharma spam was cut off, which reduced the volume of spam.

The decline in spam, however, should not be confused with a decline in risk.

"Spam volumes are not really tied to risk exposure," Landesman said. "Spam filters do an excellent job of keeping the stuff out people’s inboxes."

She added that as a result of good spam filters, spam isn’t as much of a risk as it once was. On the other hand, the Cisco report points to a number of new trends in 2010 that due put users at risk.

Over the course of 2010, Adobe’s PDF products were attacked and updated multiple times. However according to Cisco’s data gathered from its ScanSafe cloud security division, Adobe PDF vulnerabilities were not the most exploited vulnerabilities during 2010.

"In 2010, exploited Java vulnerabilities outpaced the exploit of Adobe Reader and Acrobat," Landesman said. "Java was 3.5 times more frequently exploited than were malicious PDFs. That really spells out the need for paying attention to what’s making the headlines but also paying attention to the types of things that aren’t making the headlines."

The shift in attacks away from PDF toward Java occurred over a 12-month period. According to Cisco, in January of 2010 Java exploits represented 1.5 percent of web malware while PDF exploits accounted for 6 percent. By November of 2010 the tables had turned with Java coming in at 7 percent and PDF malware at only 2 percent.

As to why attackers shifted from PDF to Java, it all has to do with opportunity.

"There were some Java vulnerabilities along with exploit code that were disclosed in the first quarter," Landesman said. "Attackers found that the attacks were working and the reason why it continued to be successful is because people were not focused on the need to patch Java."

Oracle updated Java at multiple points throughout 2010. What’s not clear is whether or not all users properly updated to the lastest patched Java updates.

"The Java patch cycle is not as finely honed as perhaps it could be," Landesman said. "There have been complaints for users that check for an update, the system says they’re updated, but they’re not actually updated."

Another Java update issue cited by Landesman is when Java is updated but it still leaves an older version installed as well, which then is still exploitable. She noted that the Java update issues could just be user error, though they are still valid concerns.

"They lead to continued exposure even if the user has attempted to patch," Landesman said. "The thing is, you really have to question how many users have really tried to patch Java."

Landesman noted that there was so much attention focused on vulnerabilities in Adobe PDF in 2009 that by 2010 everyone was looking for them and making sure they were patched. In contrast there was no such focus on Java.

"Users still weren’t looking at Java and it just left this open potential for attackers to come and take advantage of the situation," Landesman said.

World ’Running Out of Internet Addresses’

The world will run out of Internet addresses "within weeks", according to one of the founding fathers of the web, a report said Friday.

Vint Cerf, who helped create the web by connecting computers using Internet Protocol (IP) addresses, said it was his "fault" that the 4.3 billion addresses created were running out, the Sydney Morning Herald reported.

"I thought it was an experiment and I thought that 4.3 billion would be enough to do an experiment," Cerf, who is Google?s vice president and "Chief Internet Evangelist", was quoted as saying in an interview.

"Who the hell knew how much address space we needed?"

In 1977, Cerf created the web protocol IPv4, which connects computers globally, as part of an experiment while working with the US Department of Defense. He said he never expected his experiment "wouldn?t end".

"It doesn?t mean the network stops, it just means you can?t build it very well," Cerf said.

IP addresses are the unique sequence of numbers assigned to each computer, website or other internet-connected devices. They are not the same as website domain names.

The overwhelming number of devices now accessing the internet means the addresses are running out fast.

To resolve the crisis, an updated protocol for the Internet, IPv6, currently being planned by the industry, will create trillions of addresses.

As Google vice president Cerf, who was in Australia to address a conference, said he thought the new chief executive of the California-based giant, Larry Page, was ready to lead the company into the future.

In a surprise move, Google announced on Thursday that co-founder Page would replace Eric Schmidt as chief executive in April.

Schmidt, 55, a former chief executive of Novell, will remain with Google as executive chairman, focusing on deals, partnerships, customers and government outreach, Google said.

He will also act as an adviser to Page, 37, who served as CEO previously, from 1998 to 2001.

Cerf said Schmidt had been chief executive for 10 years - "a nice round number" - and Page was ready to lead the company into the future.

"Larry and Sergey are 10 years older than they were when they thoughtfully hired Eric to be the CEO... so everybody’s growing up," Cerf said.

Google has grown over the past decade from a start-up battling other Internet search engines into a technology giant with nearly 25,000 employees and annual revenue of nearly $30 billion.

The company meanwhile reported its fourth-quarter net profit increased to $2.54 billion from $1.97 billion a year ago, while revenue rose 26 percent to $8.44 billion.

107 Trillion Emails Sent Last Year

Internet users sent a total of 107 trillion emails last year, most of them spam, according to a Web monitoring service.

The number of emails sent last year were among the facts and figures about the Internet gathered by Pingdom from various sources and published Thursday at royal.pingdom.com/2011/01/12/internet-2010-in-numbers/.

Pingdom said that as of June 2010, there were 1.97 billion Internet users: 825.1 million in Asia, 475.1 million in Europe, 266.2 million in North America, 204.7 million in Latin America and the Caribbean, 110.9 million in Africa, 63.2 million in the Middle East and 21.3 million in Oceania and Australia.

Pingdom said an average of 294 billion email messages were sent per day and about 89 percent were spam.

It said there are 2.9 billion email accounts worldwide and 152 million blogs.

The total number of websites is 255 million, Pingdom said, up 21.4 million over the previous year.

It said there were 88.8 million .com domain names, 13.2 million .net domain names, 8.6 million .org domain names and 79.2 million country code domains such as .cn or .uk.

Pingdom also published figures on the growth of Twitter and Facebook.

Twitter added 100 million new accounts last year and had a total of 175 million as of September, Pingdom said, adding that 25 billion messages, or "tweets," were sent in 2010.

Facebook had nearly 600 million users at the end of the year with 250 million joining in 2010.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.